Daily threat bulletin

1 May 2024

Vulnerabilities

R language flaw allows code execution via RDS/RDX files

BleepingComputer - 30 April 2024 15:46

A new vulnerability has been discovered in the R programming language that allows arbitrary code execution upon deserializing specially crafted RDS and RDX files. [...]

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.CVE-2024-29988 Microsoft SmartScreen Prompt Security Feature Bypass Vulnerability.

Threat actors and malware

New Latrodectus malware attacks use Microsoft, Cloudflare themes

BleepingComputer - 30 April 2024 19:08

Latrodectus malware is now being distributed in phishing campaigns using Microsoft Azure and Cloudflare lures to appear legitimate while making it harder for email security platforms to detect the emails as malicious. [...]

New Wpeeper Android malware hides behind hacked WordPress sites

BleepingComputer - 30 April 2024 13:41

A new Android backdoor malware named 'Wpeeper' has been spotted in at least two unofficial app stores mimicking the Uptodown App Store, a popular third-party app store for Android devices with over 220 million downloads. [...]

Attackers Planted Millions of Imageless Repositories on Docker Hub

darkreading - 30 April 2024 21:45

The purported metadata for each these containers had embedded links to malicious files.

To Damage OT Systems, Hackers Tap USBs, Old Bugs & Malware

darkreading - 30 April 2024 18:28

USBs have something the newest, hottest attack techniques lack: the ability to bridge air gaps.